



Daily Open Source Infrastructure Report 24 September 2012

Top Stories

- A federal cybersecurity team issued a warning to customers of ORing Industrial Networking control devices about a serious vulnerability that exposes their organizations to cyberattacks. – *Softpedia* (See item [1](#))
- Dell SecureWorks researchers discovered a cyber espionage campaign targeting several large companies, including two in the energy sector. – *ComputerWeekly.com* (See item [4](#))
- Heavy rain and strong winds hammered Mat-Su Borough, Alaska, prompting many flood advisories and road closures, including an incident where 10 people were rescued in Wasilla. – *KTUU 2 Anchorage* (See item [17](#))
- A brawl at a Tucson, Arizona prison involving 200 inmates seriously injured 3 inmates, and hurt 8 other prisoners, and 3 corrections officers. – *Associated Press* (See item [33](#))
- Wildfires in central Washington merged and tripled in size to more than 47 square miles, as thousands of firefighters struggled to contain blazes that forced evacuations of hundreds of homes. – *Associated Press* (See item [48](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
 - [National Monuments and Icons](#)
-

Energy Sector

1. *September 21, Softpedia* – (International) **Flawed ORing networking devices expose oil and gas companies to cyberattacks.** DHS' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory to warn customers of ORing Industrial Networking devices of a serious vulnerability that exposes their organizations to cyberattacks, Softpedia reported September 21. A remote attacker who knows the hard-coded credentials can exploit the affected product by logging into the device with administrative privileges. This gives him/her permission to change the system's settings, and even read and write files. "An attacker can log into the operating system of the device using an SSH connection with the root credentials to gain administrative access. Once the attacker gains access to the device, the file system and settings can be accessed, which could result in a loss of availability, integrity and confidentiality," ICS-CERT reports. The products susceptible to such attacks are industrial serial device servers and they are used for SCADA systems.
Source: <http://news.softpedia.com/news/Flawed-ORing-Networking-Devices-Expose-Oil-and-Gas-Companies-to-Cyberattacks-293994.shtml>
2. *September 21, Associated Press* – (Wyoming) **Kinder Morgan to pay \$316,000 over 2 Wyo. plants.** Federal regulators say Kinder Morgan Upstream LLC has agreed to pay \$316,000 for violating risk management plan provisions at its natural gas plants in Casper and Douglas, Wyoming. The U.S. Environmental Protection Agency (EPA) said September 20 the company has agreed to establish new operating procedures, improve equipment maintenance, and perform tests to reduce the possibility of accidental releases of hazardous chemicals at both facilities. Kinder Morgan said it has taken all necessary corrective actions to address the 2011 EPA violations it received to ensure such issues do not occur again. The Clean Air Act requires facilities with hazardous and flammable substances above certain thresholds to develop risk management plans. EPA inspectors said Kinder Morgan had not adequately implemented those regulations at the Casper and Douglas plants.
Source: <http://www.businessweek.com/ap/2012-09-21/kinder-morgan-to-pay-316-000-over-2-wyo-dot-plants>
3. *September 20, KJRH 2 Tulsa* – (Oklahoma) **Train carrying coal derails south of Muskogee.** Sheriff's deputies responded to a train derailment south of Muskogee, Oklahoma, September 20. The sheriff said a train carrying coal was on fire after derailling near Old Highway 69 and 93rd Road. A total of 31 train cars were involved. Oktaha Road between Oktaha and Muskogee was closed due to the accident. The sheriff said the fire department was bringing in a special apparatus from Texas to help put out the flames, which sparked a grass fire nearby, but the fire has since been extinguished. The cause of the derailment was not immediately known.
Source: http://www.kjrh.com/dpp/news/local_news/muskogee/train-carrying-coal-derails-south-of-muskogee
4. *September 20, ComputerWeekly.com* – (International) **Dell SecureWorks uncovers cyber espionage targeting energy firms.** Dell SecureWorks researchers discovered a

cyber espionage campaign targeting several large companies, including two in the energy sector, ComputerWeekly.com reported September 20. The campaign, dubbed Mirage, targeted an oil company in the Philippines, an energy firm in Canada, a military organization in Taiwan and other unidentified targets in Brazil, Israel, Egypt, and Nigeria. This is the second cyber espionage campaign to be uncovered during 2012 by the Counter Threat Unit of security firm Dell SecureWorks. The first campaign, dubbed Sin Digoo, targeted several petroleum companies in Vietnam, government ministries in different countries, an embassy, a nuclear safety agency, and other business related groups. The Dell SecureWorks researchers believe either the same group is behind both campaigns, or whoever is responsible for Mirage is working closely with those behind Sin Digoo.

Source: <http://www.computerweekly.com/news/2240163620/Dell-SecureWorks-uncovers-cyber-espionage-targeting-energy-firms>

5. *September 20, Des Moines Register* – (Iowa) **Jefferson oil spill one of Iowa's largest; EPA takes over investigation.** An oil spill in Jefferson, Iowa, appears to be the largest in Iowa history, and the U.S. Environmental Protection Agency (EPA) has taken over the investigation, the Iowa Department of Natural Resources (DNR) said. Crews have found oil along 10-15 miles of the North Raccoon River, but have not determined how much oil spilled from a 20,000-gallon above ground storage tank at Krieger's Greenhouses. The Greene County sheriff's department reported the spill September 13. Oil ran out of a tank valve, down a ravine, through a culvert and into the river, which provides drinking water for the Des Moines area. A DNR environmental specialist said cleanup crews used vacuum trucks, skimmers, booms, and absorbent pads to recover the product, which is being tested to see if it also contained pesticides or other chemicals. So far, 800 gallons of oil and 1,000 gallons of mixed oil and water have been recovered. DNR warned residents to stay out of the river. No water supplies have been contaminated. There has been no evidence of a fish kill, though crews found two birds contaminated with oil.
Source: <http://blogs.desmoinesregister.com/dmr/index.php/2012/09/20/jefferson-oil-spill-may-be-iowas-largest-epa-takes-over-investigation/>
6. *September 19, Reuters* – (International) **BP shuts down Norwegian oil field after leak.** British Petroleum (BP) shut a Norwegian oil and gas field after a potentially dangerous leak, the company said September 17, 6 days after the incident forced the emergency shutdown of the facility. "A substantial escape of hydrocarbons occurred on the Ula field in the Norwegian North Sea on 12 September," the Petroleum Safety Authority Norway (PSA) said. "The PSA considers the incident to have had a substantial potential. The leak arose in the separator module on Ula's production platform," it added. BP said it shut the field and will not resume production until "the causes of the incident have been clarified and the conditions rectified."
Source: <http://insideclimatenews.org/todaysnews/20120919/bp-shuts-down-norwegian-oil-field-after-leak>
7. *September 19, Contra Costa Times* – (California) **'I just decided to run,' one witness says of Martinez gas station fire.** Witnesses described a frightening scene September 19 at a gas pump fire that was quickly extinguished before it damaged anything more

than cars and a gas station in Martinez, California. Nobody was injured in the fire, and officials were still investigating what caused the crash. The roof above the pumps also was damaged. Fire hoses were stretched across all four lanes of Alhambra Avenue, and the smoke initially was very dense, police said. The driver of the car that crashed into the pump was detained by police but was not immediately placed into custody. Police said they were in the initial stages of the investigation. A clerk inside the gas station market saw the crash, and quickly hit an emergency cut off button, stopping the flow of gas. Firefighters arrived and used foam to extinguish the fire in about 15 minutes, said the battalion chief of the Contra Costa Fire Protection District.

Source: http://www.contracostatimes.com/news/ci_21586318/crews-responding-fire-at-martinez-gas-station?source=most_viewed

For more stories, see items [39](#) and [45](#)

[\[Return to top\]](#)

Chemical Industry Sector

8. *September 20, U.S. Department of Labor* – (Ohio) **U.S. Labor Department’s OSHA cites OPC Polymers in Columbus, Ohio, for process safety management program deficiencies; fines exceed \$138,000.** The U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) cited Yenkin Majestic Paint Corp. for 26 health violations September 20, after a cloud containing flammable vapors was released from the company’s Columbus, Ohio facility, which operates as OPC Polymers, March 21. Proposed fines total \$138,600. The vapor cloud was caused by a copolymer reaction of flammable chemicals when over-pressurization occurred in the equipment, OSHA found after its inspection of the plant that employs about 190 people. “It is clear that OPC Polymers failed to create safety procedures, and did not train and review procedures with employees to ensure their effectiveness,” said OSHA’s area director in Columbus. Twenty-five serious safety violations relate to process safety management, including incomplete process safety information that lacked accurate piping and instrument diagrams or design codes and standards.

Source:

http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23010

9. *September 20, Associated Press* – (Louisiana) **Vinyl chloride maker hit with OSHA fines.** A chemical company in Geismar, Louisiana, that makes vinyl chloride was hit with fines for safety and health violations, September 20. The U.S. Department of Labor’s Occupational Safety and Health Administration cited the Westlake Vinyls Co. for 10 violations. The fines total \$67,000. The acting director for OSHA in Baton Rouge, said Westlake Vinyls “exposed its employees to avoidable workplace hazards that can cause serious injury and possible death.” The violations involve, among other problems, safety issues with piping and instrument diagrams, emergency shutdown procedures, and pressure-relieving devices. The company produces vinyl chloride monomer and polyvinyl chloride. There are about 140 workers at the plant. In March the facility was damaged by an explosion and fire.

Source: <http://www.vcstar.com/news/2012/sep/20/vinyl-chloride-maker-hit-with-osha-fines/>

For another story, see item [35](#)

[\[Return to top\]](#)

Nuclear Reactors, Materials and Waste Sector

10. *September 21, Reuters* – (Idaho) **Idaho wildfire roars through former uranium mine site.** A wildfire in east-central Idaho burned through three former mining sites containing traces of radioactive thorium and uranium and was advancing towards a fourth such site September 20, but State officials said they believed the risk to human health was low. As a precaution, environmental authorities planned to take air samples in North Fork, a small community in the fire zone north of Salmon, to assess any radioactive hazards posed by fire damage to the sites. One area of concern was a defunct uranium mine and milling operation 5 miles west of North Fork, where the U.S. Environmental Protection Agency conducted a cleanup several years ago of polluted soil, hazardous wastes, and piles of raw uranium and thorium ore. No decontamination of buildings at that site was ever performed, and at least one of those buildings burned in the fire, according to officials from the Idaho Department of Environmental Quality. Flames also swept two abandoned gold mines about 20 miles west of North Fork, where surface radiation, presumably from natural uranium and thorium deposits in the ground, has been measured at several times normal background levels, officials said. Source: <http://www.reuters.com/article/2012/09/21/us-usa-wildfires-idINBRE88K06320120921>

11. *September 21, WGAL 8 Lancaster* – (Pennsylvania) **TMI officials identify cause of plant shutdown.** The Three Mile Island (TMI) nuclear power plant in Londonderry Township, Pennsylvania, experienced an automatic shutdown September 20, plant officials said. A TMI spokesman said there was a problem with a reactor coolant pump that helps to circulate water through the reactor coolant system. When the pump shut down, that triggered the plant to automatically shut down. Officials said the amount of radiation released was so small it was not measurable. A plant spokesperson said there was no health risk and the public was not in danger. Source: <http://www.wgal.com/news/susquehanna-valley/dauphin/TMI-officials-identify-cause-of-plant-shutdown/-/9704162/16679486/-/8whfdoz/-/index.html>

[\[Return to top\]](#)

Critical Manufacturing Sector

12. *September 21, Reuters* – (National) **GM recalling almost 474,000 cars over problem with gear shift.** General Motors Co (GM) announced September 21 the recall of 473,841 model year 2007-2010 Chevrolet Malibu, Pontiac G6, and Saturn Aura vehicles globally to fix a condition that could lead the cars to roll when the drivers think they are in park. GM said it was aware of four crashes that resulted from the

problem, but no injuries. The company said the recall affected vehicles equipped with four-speed automatic transmissions. GM will repair the condition in which the transmission gear position may not match the gear on the shifter. Dealers will reinforce the shift cable end fitting to prevent that part from fracturing, GM said. Owners will be notified by letter to schedule the free repairs at dealers, and those who have had the work done already will be eligible for reimbursement.

Source: <http://bottomline.nbcnews.com/news/2012/09/21/14009262-gm-recalling-almost-474000-cars-over-problem-with-gear-shift?lite>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Banking and Finance Sector

13. *September 20, U.S. Securities and Exchange Commission* – (International) **SEC freezes assets of insider trader in Burger King stock.** The Securities and Exchange Commission (SEC) September 20 obtained an emergency court order to freeze the assets of a stockbroker who used nonpublic information from a customer and engaged in insider trading ahead of Burger King's announcement it was being acquired by a New York private equity firm. The SEC alleges the stockbroker, a citizen of Brazil who was working for Wells Fargo in Miami, learned about the impending acquisition from a brokerage customer who invested at least \$50 million in a fund managed by private equity firm 3G Capital Partners Ltd. and used to acquire Burger King in 2010. The broker misused the confidential data to illegally trade in Burger King stock for \$175,000 in illicit profits, and he tipped others living in Brazil and elsewhere who also traded on the information. The SEC obtained an asset freeze. It took the emergency action to prevent the broker from transferring his assets outside of U.S. jurisdiction. He recently abandoned his most current job at Morgan Stanley Smith Barney, put his Miami home up for sale, and began transferring all of his assets out of the country.

Source: <http://www.sec.gov/news/press/2012/2012-195.htm>

14. *September 20, Associated Press* – (Oregon) **SEC files fraud charges against Ore. fund manager.** The Securities and Exchange Commission (SEC) September 20 filed fraud charges against an Oregon man accused of running a Ponzi scheme that raised more than \$37 million. The SEC alleges that the man from Grifphon Asset Management in Lake Oswego falsely boasted of double-digit returns to lure more than 100 people to invest their money in hedge funds he managed. He then used money to pay off earlier investors and pay for his personal expenses and travel. The complaint filed in federal court claims little of the money was invested. He allegedly created phony assets and sent bogus account statements to investors.

Source: <http://www.sfgate.com/news/article/SEC-files-fraud-charges-against-Ore-fund-manager-3881299.php>

Transportation Sector

15. *September 21, Associated Press* – (Missouri) **2 fatal crashes close Interstate 70 in suburban KC.** The driver of a motor-assist vehicle has died while responding to a fatal crash on Interstate 70 in suburban Kansas City, Missouri. Authorities said a section of I-70 was closed September 21. KMBC 6 Kansas City reported that in the first crash, two people were ejected from their vehicles, and one of them died. Emergency crews were at the scene of that crash when a vehicle hit a motor-assist truck, causing it to burst into flames. The motorist-assist driver was hit outside his vehicle and died at the scene. The driver who hit the motor-assist truck was taken to a hospital with serious injuries.
Source: <http://www.sacbee.com/2012/09/21/4841045/2-fatal-crashes-close-interstate.html>
16. *September 21, Johnson City Press* – (Tennessee) **Two students requiring surgery at JCMC from Thursday bus wreck ‘came through fine’.** Twelve victims from a September 20 Washington County, Tennessee bus crash were in stable condition September 21, according to a hospital’s communications manager. The status of eight students treated at another hospital was unclear, but the communications manager said she would have an update September 21. Tennessee Highway Patrol investigators were expected back at the scene on Mt. Wesley Road September 21 to gather more information about the crash. Twenty-seven people were injured in all when the bus they were on crashed and flipped over. The bus was taking students home from David Crockett High School.
Source:
<http://www.johnsoncitypress.com/News/article.php?id=102489#ixzz2771UeDUQ>
17. *September 20, KTUU 2 Anchorage* – (Alaska) **Mat-Su floods, road closures: 10 people rescued in Wasilla.** Heavy rain and strong winds continued to hit the Mat-Su Borough prompting many flood advisories and road closures, including an incident where 10 people were rescued in Wasilla, Alaska, September 20. A flash flood swept through a neighborhood off of Lucille Street and Marilyn Circle. Residents of the house with the most flooding said the water rose so fast that by the time they pulled out of their driveway, the water was waist deep. People who lived in the four other homes were rescued by emergency responders who rafted them to safety. Mat-Su Borough officials said Shorty Road and Welch Road were closed. It said rock slides increased between Miles 77 and 79 on the Glenn Highway, west of where it crosses the Chickaloon River. Borough officials noted that Talkeetna, Beaver, and Mercedes roads were flooded, and in East Talkeetna, people were instructed to evacuate immediately at the north end of Beaver Road. Three shelters opened overnight, according to the American Red Cross of Alaska.
Source: http://articles.ktuu.com/2012-09-20/mat-su-borough_33984261
18. *September 20, Associated Press* – (Louisiana) **Bomb threat at Baton Rouge airport.** The terminal at Louisiana’s Greater Baton Rouge Metro Airport in Baton

Rouge reopened about 3 hours after authorities evacuated it because of a bomb threat September 20. An airport spokesman said airport resumed normal operations early in the evening. In the late afternoon September 20, the terminal and parking garage were evacuated and a perimeter was set up around the airport to keep people out. Authorities said passengers on a plane that landed just before the bomb threat waited on the aircraft.

Source: <http://www.knoe.com/story/19600443/bomb-threat-at-baton-rouge-airport>

For more stories, see items [3](#) and [45](#)

[\[Return to top\]](#)

Postal and Shipping Sector

19. *September 20, WISH 8 Indianapolis* – (Indiana) **Police make arrest after mailbox thefts.** Police believe they nabbed the person behind multiple mailbox thefts in Johnson County, Indiana. She was arrested September 17 in Hancock County after being pulled over for speeding through a school zone; there was a warrant out for her arrest. Police said at least five people in Johnson County reported in August they had checks taken from their mailboxes. Those checks had been written out to pay bills, but then were cashed for hundreds of dollars. An official from the Johnson County Sheriff's Department said the locations where the checks were cashed caught the suspect on video. They said she used her own valid driver's license as well. Police put out a warrant for her arrest. Police believed there may be other victims in other counties. They said their investigation was continuing.

Source: <http://www.wishtv.com/dpp/news/indiana/police-make-arrest-after-mailbox-thefts>

[\[Return to top\]](#)

Agriculture and Food Sector

20. *September 21, Occupational Health & Safety* – (National) **FSIS issues new Salmonella guide for small entities.** The Food Safety and Inspection Service (FSIS) issued a revised compliance guide that will help small and very small meat and poultry establishments produce ready-to-eat products with respect to Salmonella and other pathogens, Occupational Health & Safety reported September 21. Posted September 19, the guide is not available in hard copy, according to the FSIS notice announcing its availability.
Source: <http://ohsonline.com/articles/2012/09/21/fsis-issues-new-salmonella-guide-for-small-entities.aspx?admgarea=ht.FoodSafety>
21. *September 21, Softpedia* – (International) **US Department of Agriculture sites hacked in protest against Mohammed movie.** Hackers from the Bangladesh Cyber Army protested against the Innocence of Muslims video by breaching three subdomains owned by the U.S. Department of Agriculture. "We are BANGLADESH CYBER ARMY, the first and largest hacking group of Bangladesh! Recently, a movie was

released where the Prophet of Islam, Hazrat Muhammad (Sm) was insulted,” the hackers told Softpedia in an email. “There was a protest regarding removal of the movie. Being a cyber army of the Muslim world, we felt necessary to join the protest. As a result, we hacked a few of US Government sites. A number of normal US sites were also hacked.”

Source: <http://news.softpedia.com/news/US-Department-of-Agriculture-Sites-Hacked-in-Protest-Against-Mohammed-Movie-293926.shtml>

22. *September 20, U.S. Food and Drug Administration* – (National) **Del Monte Fresh Produce N.A. Inc, recalls limited quantity of fresh cut mango products due to possible health risk.** In cooperation with the Food and Drug Administration’s warning to not consume mangoes from Agricola Daniella in Mexico, Del Monte Fresh Produce N.A., Inc, September 20 initiated a voluntary recall of 1,600 bowls of fresh-cut mangoes distributed to retail outlets due to the potential risk that the mangoes may contain Salmonella. This recall is associated with FoodSource’s (Edinburg, Texas) recall of mangoes sourced from Agricola Daniella in Mexico. Product was distributed between September 8-12 by retailers in the states of Florida, Georgia, North Carolina, Oregon, South Carolina, Tennessee, and Washington. Product is packaged in clear plastic 32-ounce. bowls with a Del Monte label on the top. The affected product will have printed best by date September 16 and lot code 05252101 below, and best by date September 22 and lot code 03256100 below. The UPC is 7-62357-07532-1.
Source: <http://www.fda.gov/Safety/Recalls/ucm320373.htm>
23. *September 20, U.S. Department of Agriculture Food Safety and Inspection Service* – (National) **FSIS issues public health alert for imported Canadian raw boneless beef trim from XL Foods.** The U.S. Department of Agriculture’s Food Safety and Inspection Service announced a public health alert September 20 for raw boneless beef trim products imported from Canada by XL Foods, Inc. that may be contaminated with E. coli O157:H7. The products subject to the recall were distributed to U.S. establishments in the following states: California, Michigan, Nebraska, Oregon, Texas, Utah, Washington, and Wisconsin. At the U.S. establishments, these products may have been further processed into various products such as ground beef, ground beef patties, beef jerky, and pastrami.
Source: http://www.fsis.usda.gov/News_&_Events/NR_092012_01/index.asp
24. *September 20, KRTV 3 Great Falls* – (Montana) **Drought continues with 13 new counties declared natural disaster areas.** With weeks of little to no rain, more than 60 percent of Montana was experiencing some severity of drought conditions, according to the National Oceanic and Atmospheric Administration (NOAA). September 20, NOAA released its’ weekly Drought Monitor, which showed no improvement for the State. As the dry weather persists, the U.S. Department of Agriculture Farm Service Agency (USDA FSA) declared 13 new counties as primary natural disaster areas. This designation allows farm operators to apply for low interest emergency loans from the USDA FSA. Those counties include Carbon, Carter, Cascade, Golden Valley, Judith Basin, Meagher, Musselshell, Park, Powder River, Stillwater, Sweet Grass, Treasure, and Wheatland. Nearby counties are also eligible for natural disaster assistance. Those include Big Horn, Broadwater, Chouteau, Custer,

Fallon, Fergus, Gallatin, Lewis and Clark, Petroleum, Rosebud, Teton, and Yellowstone.

Source: <http://www.krtv.com/news/drought-continues-with-13-new-counties-declared-natural-disaster-areas/>

[\[Return to top\]](#)

Water Sector

25. *September 21, Odenton-Severn Patch* – (Maryland) **Army to remove soil from pesticide shop site.** The U.S. Army plans to excavate more than 700 tons of dirt from the site of a former pesticide shop at Fort Meade, Maryland, after it found contamination in the soil and groundwater. A geologist with Arcadis, an environmental services firm said the pollution does not pose any direct risk to anyone on base, but it could threaten the health of any workers who might construct buildings at the location. Work could begin as soon as the spring. From 1958 to 1978, the former shop was used as a maintenance facility for landscaping equipment and housed pesticides. From 1997 to 2010, the Army conducted field tests to determine the level of pollution in the soil and groundwater which revealed elevated levels of arsenic, pesticides, and volatile organic compounds. The Army put together a feasibility study earlier this year to prevent human exposure to pollutants and to clean up the groundwater. The Army, U.S. Environmental Protection Agency, and Maryland Department of Environment recommended excavating the site. The plan would also mean injecting groundwater with emulsified vegetable oil, which speeds up natural biodegradation. The Army will also continue monitoring the water for about 10 years.

Source: <http://odenton.patch.com/articles/army-to-remove-soil-from-former-pesticide-shop>

26. *September 21, Fredericksburg Free-Lance Star* – (Virginia) **Caroline campground faces \$10k fine.** Four Winds Campground in Caroline County, Virginia, faces a \$10,500 fine for problems associated with its sewage treatment plant, the Fredericksburg Free-Lance Star reported September 21. That is according to a proposed consent order between Caroline County campground owner Four Winds Club Inc. and the State Water Control Board. The order said the campground near Woodford reported it exceeded its permit limit for ammonia discharge due to equipment problems. The plant makes intermittent discharges of treated sewage into the Rappahannock River. In addition, a report on the integrity of a discharge pipe was filed 3 months late, and without required photographs, said the order. Also, a dye test was not performed, and a separate groundwater-monitoring report was 2 months late. Four Winds agreed to conduct a dye test and inspect the discharge pipe for leaks. And it must submit a plan and schedule to address the ammonia violations to the Virginia Department of Environmental Quality. The State Water Control Board will take up the matter after a public comment period ends.

Source: <http://blogs.fredericksburg.com/carolinecrossroads/2012/09/21/caroline-campground-faces-10k-fine/>

27. *September 20, Galesburg Register-Mail* – (Illinois) **Lightning plagues Galesburg sewer plant.** The Galesburg, Illinois Sanitary District superintendent reported September 20 that about five or six major lightning strikes have occurred at the water treatment plant, causing concern for officials. Officials could not conclude what makes the plant so conducive to lightning strikes. Water tanks and transformers could be one reason, but that does not explain the occurrence of ground strikes at the site as well. The director of engineering and maintenance said an August 18 strike hit a transformer at the treatment plant, causing significant damage to the transformer and other equipment; so far repair costs exceed \$5,000.
Source: <http://www.galesburg.com/news/x1547509835/Lightning-plagues-Galesburg-sewer-plant>
28. *September 20, BrownwoodNews.com* – (Texas) **Texas Water Development Board approves \$12M for Brownwood Wastewater Treatment Plant.** The Texas Water Development Board (TWDB) September 20 approved \$12 million to the city of Brownwood in loans from the Texas Water Development Fund to finance wastewater system improvements. The city intends to use the funds to make improvements to its wastewater treatment plant and the Slayden Street Lift Station, and is proposing the development of a supplemental water supply treatment facility for direct potable reuse. Officials said improvements to the existing wastewater treatment plant are necessary.
Source: http://www.brownwoodnews.com/index.php?option=com_content&view=article&id=9707:texas-water-development-board-approves-12m-for-brownwood-wastewater-treatment-plant&catid=35:news&Itemid=58

For another story, see item [5](#)

[\[Return to top\]](#)

Public Health and Healthcare Sector

29. *September 20, Florida Times-Union* – (Florida) **Temporary lockdown at Jacksonville hospital after gun was fired.** A patient fired a gun September 20 in a second-floor room at St. Vincent's Medical Center Riverside in Jacksonville, Florida, but no one was injured, according to the Jacksonville Sheriff's Office. The private hospital went on lockdown after the patient grabbed the handgun from his wife's purse when she was out of the room. The patient was "completely disoriented" as he fired off a round that went through a wall, said a sheriff's office spokeswoman. St. Vincent's HealthCare policy prohibits firearms on hospital grounds. A hospital spokeswoman said they believed that the woman had a permit for the gun. Police did not believe any criminal intent was involved.
Source: <http://jacksonville.com/news/crime/2012-09-20/story/temporary-lockdown-jacksonville-hospital-after-gun-was-fired>
30. *September 19, Threatpost* – (Massachusetts) **Massachusetts hospital agrees to pay \$1.5m after stolen laptop HIPAA violation.** Massachusetts Eye and Ear Infirmary (MEEI), a Boston-based hospital, agreed to pay \$1.5 million to the U.S. Department of

Health and Human Services (HHS) September 17, settling a HIPAA violation stemming from a 2010 incident. Two years ago, while a doctor was traveling abroad, his unencrypted laptop — containing information on roughly 3,500 patients, including patients' prescriptions and other clinical information — was stolen. According to an alert then, the laptop contained no billing data but did contain patients' names, addresses, telephone numbers, emails, and other identifiable information. While it was never confirmed any patients had their information breached, the hospital informed HHS of the incident and an investigation was initiated. The investigation found the hospital failed to comply with six areas of HIPAA between October 2009 and June 2010. MEEI failed to "implement security measures sufficient to ensure the confidentiality of electronic protected health information" and "conduct a thorough analysis of the risk to the confidentiality of electronic protected health information maintained on portable devices," among other steps, said a press release. Besides the fine, MEEI must also follow a new Corrective Action Plan that outlines steps to ensure it complies with HIPAA, perform risk assessment, and train its staff. It must also submit to semi-annual audits for 3 years.

Source: http://threatpost.com/en_us/blogs/massachusetts-hospital-agrees-pay-15m-after-stolen-laptop-hipaa-violation-091912

[\[Return to top\]](#)

Government Facilities Sector

31. *September 20, KAIT 8 Jackson* – (Arlington) **Caraway man charged with attacking children at elementary school.** The Caraway Police Department is investigating an incident between a parent and students at Riverside Elementary School in Caraway, Arkansas. A Craighead County judge charged a Caraway resident with three counts of second degree battery, three counts of false imprisonment, and one count of first degree terroristic threatening after Caraway police said he attacked three third graders in a classroom September 18. The Riverside Public Schools superintendent said the man was at the school because he had eaten lunch with his daughter. He said the man went into a classroom during the students' transition from lunch back to class to confront a student the man believed had mistreated his daughter. The man prevented three students from leaving a classroom with the intention of targeting one of the students, and all three students were injured during the incident, according to police. The superintendent said the man choked the child he thought was mistreating his daughter. Source: <http://www.kait8.com/story/19586085/man-allegedly-attacks-children-at-elementary-school>
32. *September 20, KTVB 7 Boise* – (Idaho) **Police investigate 'hit list' at Homedale High.** Officers were called to Homedale High School in Homedale, Idaho, September 20 due to a reported "hit list" that was identified or found somewhere in the school. The Homedale superintendent told KTVB 7 Boise that all students were safe, and that classes were still in session. He also said an unidentified student had been suspended for 15 days due to the incident. Police said there were more than a dozen names on the hit list. September 19, students and parents received an email from the Homedale School District explaining the problem, and informing students that it was safe to come

to class.

Source: <http://www.ktvb.com/home/Police-investigate-hit-list-at-Homedale-High-170516766.html>

For more stories, see items [25](#), [45](#), and [48](#)

[\[Return to top\]](#)

Emergency Services Sector

33. *September 21, Associated Press* – (Arizona) **Fight involving 200 at Ariz. prison leaves 14 hurt.** Two or three corrections officers were among those treated after a fight broke out among 200 black and Hispanic inmates at a State prison complex in Tucson, Arizona, September 20. The brawl broke out in a recreation yard at the prison's Santa Rita unit, an Arizona Department of Corrections spokesman said. It was broken up by a prison tactical force using pepper spray and "minimal force" within a half hour, the spokesman said. One of the inmates was in critical condition September 21, a hospital spokesman said, and two others were in the intensive care unit in serious condition. The hospital treated and released three prison guards. The corrections spokesman said the melee injured two officers and 11 inmates. The prison has 5,150 beds and the unit where the fight broke out houses 727 inmates.

Source: <http://www.charlotteobserver.com/2012/09/21/3545307/scores-of-inmates-fight-at-ariz.html>

34. *September 21, Associated Press* – (International) **3 killed in inmate hunt shootout near US border.** Authorities in Mexico said three gunmen have been killed after attacking police hunting for inmates who joined in a mass escape from a prison near the U.S. border. The Coahuila state prosecutor's office said the gunmen were in a truck in a residential area of the border city of Piedras Negras when they fired on state police officers September 20 who were helping look for some of the 131 prisoners who fled a nearby prison earlier the week of September 17. Investigators have yet to determine whether the dead gunmen were escapees. The statement said the truck matches records of a vehicle stolen in San Antonio. Authorities said the Zetas drug cartel orchestrated the prison break apparently with the help of prison personnel. Three escapees have been recaptured so far.

Source: <http://www.wtnh.com/dpp/news/international/3-killed-in-inmate-hunt-shootout-near-US-border> 25957422

35. *September 20, WSBT 22 South Bend* – (Indiana) **Firefighters say next evacuation will be smoother.** It is something most Mishawaka, Indiana Firefighters have said they never had to do until September 14, WSBT 22 South Bend reported September 20. Firefighters battling a chemical fire that prompted a leak focused on canvassing nearby neighborhoods and getting people who might be in danger out of their homes. WSBT 22 South Bend was able to get that information from dispatch and get it out to the general public, but when it came to getting out specifics — the seriousness of the threat, what they were dealing with, what would happen next — it took more than 3 hours from the original dispatch until the first news conference. Another

communication flaw the battalion chief said he would fix — delegating the St. Joseph County Emergency Management director a bigger role.

Source: http://articles.wsbt.com/2012-09-20/evacuation-zone_33984276

[\[Return to top\]](#)

Information Technology Sector

36. *September 21, The H* – (International) **Apple closes security holes in Mac OS X and Safari.** Apple released updates for versions 10.6 (Snow Leopard), 10.7 (Lion), and 10.8 (Mountain Lion) of its Mac OS X operating system that close many critical security holes. Mac OS X 10.8.2, 10.7.5, and Security Update 2012-004 for Mac OS X 10.6.8 address a wide range of vulnerabilities. These include information disclosure and denial-of-service (DoS) problems, bugs in the sandbox that could allow malware to bypass restrictions, memory corruption bugs, and buffer and integer overflows. According to Apple, many of these could be exploited by an attacker to cause unexpected application termination or arbitrary code execution. Among the changes in the updates are new versions of Apache, the BIND DNS server, International Components for Unicode, the kernel, Mail.app, PHP, Ruby, and the QuickTime media player, all of which correct security problems. Apple also released an update to its Safari Web browser, version 6.0.1 that addresses multiple information disclosure vulnerabilities, including one that could allow Autofill contact data to be sent to maliciously crafted Web sites. The majority of the holes closed in Safari were memory corruption bugs found in its WebKit browser engine that could, for example, be exploited by an attacker to cause unexpected application termination or arbitrary code execution. For an attack to be successful, a victim must first visit a specially crafted Web site.

Source: <http://www.h-online.com/security/news/item/Apple-closes-security-holes-in-Mac-OS-X-and-Safari-1714236.html>

37. *September 21, The Register* – (International) **Microsoft issues emergency IE bug patch.** Microsoft released a patch that fixes five vulnerabilities, including the zero-day flaw that is cracking Windows systems via the most common versions of Internet Explorer (IE). The MS12-063 update provides a fix for the flaw, which is in use by hackers against some companies. The patch also has four more flaw fixes, which have not been spotted in the wild, said Microsoft. The flaw was rated as critical or moderate risk, depending on which browser and operating system a user is running, but would allow full remote code execution on systems running IE 7,8, and 9 running Adobe Flash on fully patched Windows XP, Vista, and 7 machines, using malware embedded in a Web page. The flaw was found by a security researcher on an Italian hacking tools site, but there were reports it has been used to distribute the Poison Ivy trojan by the same group that exploited the Java zero-day flaw found in the last month.

Source: http://www.theregister.co.uk/2012/09/21/microsoft_patches_zero_day_flaw/

38. *September 20, Infosecurity* – (International) **IBM: Top threats include data breaches, BYOD, browser exploits.** When it comes to trends in security for 2012 so far, the landscape has seen a sharp increase in browser-related exploits, like recent ones for

Internet Explorer and Java, along with renewed concerns around social media password security and continued disparity in mobile devices and corporate bring-your-own-device (BYOD) programs. That information comes from the IBM X-Force 2012 Mid-Year Trend and Risk Report, which shows that a continuing trend for attackers is to target individuals by directing them to a trusted URL or site injected with malicious code. Through browser vulnerabilities, the attackers are able to install malware on the target system. Further, the growth of SQL injection, a technique used by attackers to access a database through a Web site, is keeping pace with the increased usage of cross-site scripting and directory traversal commands.

Source: <http://www.infosecurity-magazine.com/view/28370/ibm-top-threats-include-data-breaches-byod-browser-exploits>

39. *September 20, Government Computer News* – (National) **Energy lab develops Sophia to help secure SCADA systems.** New cybersecurity software developed by an Energy Department lab specifically for utilities and other industrial systems could be available as early as October. The Idaho National Laboratory’s Sophia software sentry, funded by the Energy Department’s Office of Electricity Delivery & Energy Reliability and DHS, passively monitors networks to help operators detect intruders and other anomalies. Industrial systems such as power plants have concentrated on physical security because they were not connected to the Internet, but that has changed as operators have added computer networks. Sophia is a tool to automate real-time monitoring on static Supervisory Control and Data Acquisition (SCADA) system networks — those with fairly fixed communications patterns. Anything out of the ordinary triggers an alert. If the program detects suspicious activity, it alerts an operator or network administrator, who can then decide if the activity is threatening.
Source: <http://gcn.com/articles/2012/09/20/inl-sophia-industrial-control-system-security-tool.aspx>

40. *September 19, Technology Review* – (International) **Stuxnet tricks copied by computer criminals.** Experts indicate the techniques used in sophisticated, state-backed malware are trickling down to less-skilled programmers who target regular Web users and their online accounts or credit card details. State-sponsored malware became widely known in 2010 with the discovery of Stuxnet, a program targeted at Iranian industrial control systems. Since then, several other very sophisticated malware packages have been discovered that are also believed to have been made by governments or government contractors. These packages include Duqu, exposed late in 2011, and Flame, found in May 2012. One reason such malware is so effective is it tends to exploit previously unknown software vulnerabilities, known as zero-days, in widely used programs such as Microsoft Windows to gain control of a computer. A Kaspersky researcher said those exploits can be quickly “copy-pasted” by other programmers, as happened after the discovery of Stuxnet. More concerning is the way higher-level design features are being picked up, he said.
Source: <http://www.technologyreview.com/news/429173/stuxnet-tricks-copied-by-computer-criminals/>

For more stories, see items [1](#), [4](#), [21](#), [30](#), [41](#), and [42](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <https://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

41. *September 20, Atlanta Journal-Constitution* – (Georgia) **AT&T customers' Internet service disrupted.** Around 7,500 AT&T customers in northern Atlanta were without Internet service for several hours September 20 after the company said it experienced a router problem. A spokesman said it would take a few days to complete an assessment of the problem, but it appeared it was caused by a defective card in a router. He said only Internet service was affected and not mobile phone service. The chief executive officer of L2Networks said the outage also affected other carriers' ability to provide similar services, including Qwest, CenturyLink, Deltacom, Earthlink, and many smaller telecommunication providers.

Source: <http://blogs.ajc.com/business-beat/2012/09/20/att-customers-internet-service-disrupted/>

42. *September 19, Computerworld* – (National) **Sprint says Virgin Mobile users are safe from account hijacks.** Sprint September 19 denied that subscribers of its Virgin Mobile subsidiary were wide open to account hijacking attacks as claimed by an independent software developer the week of September 17. In emailed comments, a Sprint spokeswoman said the company has multiple safeguards to protect customer accounts from intrusion and tampering by unauthorized users. She was responding to questions that arose from a September 17 blog post by a developer. In it, he detailed how the username and password system used by Virgin Mobile to let users access their accounts online was inherently weak and open to abuse. Virgin forces subscribers to use their phone numbers as their username and a six-digit number as their password, he noted. The developer said he went public with his discovery because Sprint did not fix the vulnerability after being told how easy it was to exploit. He also noted in his blog that Virgin Mobile subscribers had no easy way to mitigate any exposure to account hijacks. In response, Sprint said it implemented a new procedure to lock out users from their accounts after four failed attempts. The developer described that move as ineffective because hackers could bypass it by making log-in attempts without sending any cookie data with the requests.

Source:

http://www.computerworld.com/s/article/9231470/Sprint_says_Virgin_Mobile_users_are_safe_from_account_hijacks

[\[Return to top\]](#)

Commercial Facilities Sector

43. *September 21, Associated Press* – (Pennsylvania) **Police: Hostage-taker surrenders in Pittsburgh.** An armed suicidal suspect who held a businessman hostage inside a downtown Pittsburgh office building for more than 5 hours September 21, who posted Facebook updates during the standoff, surrendered to police. The hostage-taking on the 16th floor of Three Gateway Center prompted an evacuation while the suspect wrote on Facebook he had “lost everything” and that people did not have to worry about him anymore. His friends urged him to end the situation peacefully. A police spokeswoman identified the hostage as owner of CW Breitsman Associates. The firm runs employee benefits programs, but it was not immediately clear why the victim was targeted. Police asked Facebook to take down the suspect’s page in hopes of steering all of his attention to negotiations. Officials described the suspect as having a military background but did not elaborate. The suspect has a criminal record that includes a guilty plea to robbery earlier this year and a minimum 6-month jail sentence.
Source: <http://www.newstimes.com/news/article/Police-Hostage-taker-surrenders-in-Pittsburgh-3883236.php>
44. *September 20, WGBA 26 Green Bay* – (Wisconsin) **Green Bay warehouse fire forces workers to flee.** A warehouse caught fire on the west side of Green Bay, Wisconsin, and nearly 100 firefighters were called-in to battle the fire. The fire broke-out in a commercial area September 20. Five people were inside the building. They were doing some construction when their torch sparked flammable material, and within minutes the space was engulfed in flames. The building was purchased 4 months ago and was used as storage space. Only a few cars were inside. Firefighters estimated the damage from the fire is about \$350,000. Nearby buildings may have suffered some heat damage.
Source: <http://www.nbc26.com/news/170551736.html>
45. *September 20, Canton Repository* – (Ohio) **Overheated light ballast forces evacuation of Canton offices.** Smoke throughout a downtown office building in Canton, Ohio, sent nearly 100 employees into the street September 20. The fire battalion chief said the trouble was caused by an overheated light ballast in a third-floor conference room. Two light fixtures melted and when employees noticed smoke, they called firefighters, he said. However no fire broke out. The building houses the Ohio Bureau of Workers’ Compensation and Chesapeake Energy. Local streets in the vicinity were briefly closed by fire trucks and ambulances from Canton and Canton township departments.
Source: <http://www.cantonrep.com/newsnow/x1334620720/Firefighters-investigate-haze-inside-Canton-office-building>
46. *September 20, Associated Press* – (Indiana) **Fire at Indy Boy Scout camp deemed suspicious.** The second fire in 2 years to hit buildings at an Indianapolis Boy Scout camp has been deemed suspicious after arson dogs detected possible accelerants. The Crossroads of America Council of the Boy Scouts immediately posted a reward of \$5,000 for information about the predawn fire September 20 at Camp Belzer. The fire destroyed the oldest building at the camp, a cabin known as the K-Hut. The 130-acre camp along Fall Creek just east of Interstate 465 is used by 40,000 scouts per year.

Source: <http://www.fox19.com/story/19600154/fire-at-indy-boy-scout-camp-deemed-suspicious>

47. *September 20, WILX 10 Onondaga* – (Michigan) **Meth lab closes downtown Lansing business.** "Materials such as tubing and bottles..." were just some of the meth-cooking materials found in the kitchen area of a break room in the Insurance Institute of Michigan offices in Lansing, Michigan, September 19. A police spokesman said officials hoped to get details from the two suspects in custody at the city jail. The suspects found by police with the meth-making materials are janitors who were working their weekly, after-hours shift at the institute. It is a business leasing a portion of the Michigan Beer and Wine Wholesalers Association building. It was a portable operation, something police call one-pot meth making, where as long as one has all of the proper materials, the drug can be made almost anywhere in 20-30 minutes. The executive director of the insurance institute, and his employees now have to work from home indefinitely. He is waiting for the health department to make sure there are no leftover fumes or material that could harm anyone.

Source: <http://www.wilx.com/news/headlines/Meth-Lab-Closes-Downtown-Lansing-Business-170576496.html>

For more stories, see items [4](#), [26](#), and [48](#)

[\[Return to top\]](#)

National Monuments and Icons Sector

48. *September 21, Associated Press* – (Washington) **Heat, winds, low moisture make Wash. fires grow.** Wildfires in central Washington merged and tripled in size to more than 47 square miles, due to a combination of warm temperatures, winds, very low humidity, and low moisture in the vegetation, the Associated Press reported September 21. The Table Mountain blaze was being fought by more than 750 firefighters and was 5 percent contained by late September 20, fire managers said. It had not burned any homes, but 161 homes north of Ellensburg and in the Liberty area are under a Level 3 evacuation, meaning residents are urged to leave, a Kittitas County sheriff said. The Table Mountain Complex was one of several wildfires burning on the eastern slopes of the Cascade Range. The largest, the Wenatchee Complex, had grown to about 65 square miles. It was 24 percent contained and was being fought by more than 2,000 firefighters. The fires were blanketing eastern Washington with smoke forcing the relocation of school and college sporting events, and dry conditions led the State to issue restrictions on logging and other industrial activities. All together, the fires had covered more than 108 square miles as of late September 20, and hundreds of people had been evacuated from their homes.

Source: http://seattletimes.com/html/localnews/2019221019_apwawashwildfires.html

49. *September 20, Associated Press* – (California) **Workers could be tested for hantavirus.** California public health officials want to survey workers at Yosemite National Park to determine whether they were exposed to a deadly mouse-borne virus, a park spokesman said September 20. The California Department of Public Health

recently proposed to take a voluntary survey of workers to contribute to the park's understanding of hantavirus and the recent disease cluster, a Yosemite National Park spokesman said. The Mariposa Gazette reported September 20 that three park workers experienced flu-like symptoms and got tested for hantavirus. A Mariposa County Health Officer told the Mariposa County Board of Supervisors at a September 18 meeting that while initial tests came up positive, a second set of tests showed the workers were not exposed to the strain that causes hantavirus pulmonary syndrome. The Yosemite National Park spokesman said there have been no confirmed or suspected cases among employees of the National Park Service or the park's concessionaire, DNC Parks and Resort. Nine people who spent time at the park this summer have been infected with the rodent-borne virus, the majority after staying at the "Signature" cabins in Curry Village. Three of them have died.

Source: http://www.mercurynews.com/breaking-news/ci_21598139/workers-could-be-tested-hantavirus

For another story, see item [10](#)

[\[Return to top\]](#)

Dams Sector

Nothing to report

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2273
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes .
Removal from Distribution List:	Send mail to support@govdelivery.com .

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.